電腦犯罪偵查講義

第　一　回

205260-1

社團法人 考友社 出版發行

電腦犯罪偵查講義　第一回

目錄

第一講　緒論

命題重點

一、電腦犯罪概述
　㈠電腦犯罪之定義
　㈡電腦犯罪之特性
　㈢電腦犯罪之種類
　㈣電腦犯罪之型態
　㈤電腦犯罪之手法
二、電腦犯罪者
　㈠電腦犯罪者之類型
　㈡電腦犯罪者之特質
　㈢電腦犯罪者－駭客
三、法律規範
　㈠普通刑法
　㈡附屬刑法
　㈢程序法適用問題
　㈣各國電腦犯罪立法
四、犯罪偵查
　㈠犯罪調查
　㈡犯罪起訴
　㈢改善方法
五、犯罪剖繪技術
　㈠剖繪原理
　㈡適用範圍
　㈢價值功能
　㈣電腦犯罪應用
六、安全技術
　㈠犯罪預防
　㈡犯罪處理
　㈢安全工具

重點整理

一、電腦犯罪概述

㈠電腦犯罪之定義：

電腦犯罪（computer crime）爲一新穎的犯罪型態，係少數人利用電腦從事各種犯罪行爲。電腦犯罪係行爲人濫用電腦（Computer Abuse），有所謂與電腦相關之犯罪（Computer-related Crime）、電腦詐欺（Computer Fraud）、電子詐欺（Electronic Fraud）、自動資料處理犯罪（Automatic Data Processing Crime）、電腦侵入（Hacking）或電腦玩家（Hacker）及電子資料處理犯罪（Electronic Data Processing）等不一而足。到目前爲止學術界雖然尚未對「電腦犯罪」下過一致的定義，然而大致上通常分爲以下說法。

1.廣義說：

持廣義說的學者認爲「與電腦有關之犯罪」（computer related crime）即稱爲電腦犯罪。若依此言，則以電腦爲犯罪工具或目的之所有犯罪行爲，均得謂之電腦犯罪。如此定義則範圍不免失之過廣，例如竊取電腦事實上僅客體不同，與傳統的竊盜犯罪型態無異，若因其偷竊客體係爲電腦而將之歸類爲電腦犯罪，則討論電腦犯罪已失去意義，而且若以此角度看待電腦犯罪，將無法精確估計犯罪數字。

2.狹義說：

持狹義見解者，認爲所謂電腦犯罪乃指「與電子資料處理有關之故意而違法的財產破壞行爲」。易言之，如故意毀損、竄改、無權使用電腦資料、程式、設備之違法破壞財產法益的「財產犯罪」才算電腦犯罪，依此定義又未免失之過狹。從電腦犯罪研究的課題與範圍觀之，除有破壞財產法益的財產罪外，尚包括破壞電腦秘密的電腦間諜罪，均非破壞財產法益，故僅將電腦犯罪界定爲財產罪，顯然並不恰當。

3.折衷說：

綜合前述定義，又有人提出折衷說，茲舉出數項以代表之：

⑴所謂電腦犯罪乃指行爲人濫用電腦或破壞電腦，而違犯具有電腦特質之犯罪行爲。

⑵所謂電腦犯罪係指以電腦爲工具，而使自己受益或使他人遭受損失之犯罪行爲。

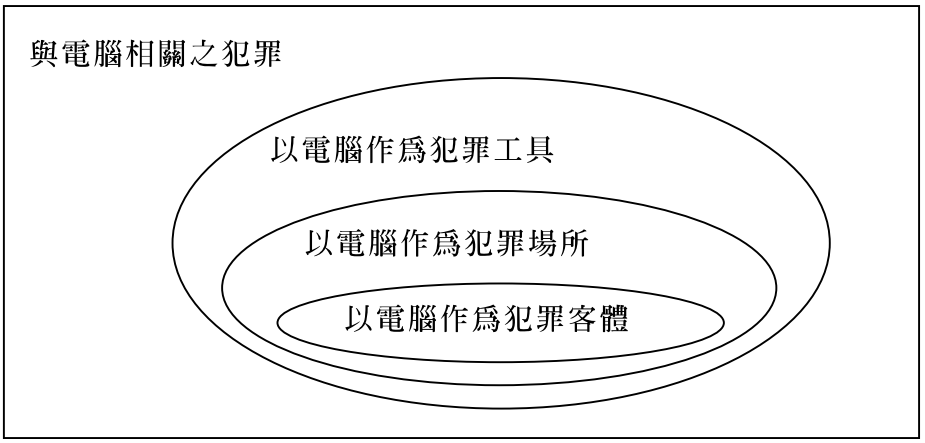
⑶所謂電腦犯罪係指以下列之目的，故意接近電腦系統或電腦網路者，均爲電腦犯罪：

①以詐欺或奪取之目的而執行程式。

②以陷他人於錯誤或詐欺之目的而獲取金錢、財產或服務。

③任何人惡意接近、改變、增減、損壞電腦系統網路或資料者。

一般而言，利用電腦特性之犯罪，依電腦在犯罪中所扮演的角色，可以分成：作爲犯罪工具、作爲犯罪場所、作爲犯罪客體（如下圖㈠）。有學者就認爲，所謂電腦犯罪是指利用電腦的特性，以電腦作爲犯罪場所，或以電腦作爲犯罪客體（攻擊目標）的犯罪行爲。所謂利用電腦之特性是指電腦具有快速隱密地儲存、處理、傳遞大量資料之功能，若非利用電腦之特性，而僅以電腦作爲犯罪的工具，則不屬於電腦犯罪。



圖㈠　電腦與犯罪的關係

若要嚴格來看，對於電腦犯罪採最狹義的定義，應只有第三類：利用電腦之特性，以電腦作爲犯罪客體的情形，才能稱爲電腦犯罪。但若採較爲廣義的定義，應將第二類也納入，因爲就偵辦犯罪與證據蒐集的角度來看，以電腦爲犯罪場所的情形，因犯罪皆是在電腦上進行和發生，電腦上的證據無可避免地對執法人員的偵辦技巧、法院的證據力認定，都形成一種新的挑戰。但就犯罪學研究而言，利用電腦的特性作爲犯罪工具，亦應納入研究範疇，方能掌握整體犯罪現象，而提出周延的解釋。

近來在報章媒體時常可見「網路犯罪」一詞，然而網路犯罪所指爲何，國內尚無學者對此加以嚴格的定義，縱有探討此一議題的論述，亦多認爲網路犯罪仍屬電腦犯罪之一環，而沿用電腦犯罪的定義。

參酌上述各學者之意見，可將凡因使用電腦而侵害電腦的軟、硬體，而謀取不法利益，在從事破壞行爲之過程中，其犯罪行爲與電腦的特質與功能有關者，即爲電腦犯罪。

㈡電腦犯罪之特性：

電腦犯罪與一般犯罪特質差異甚大，在此將其特性敘述如下：

1. 白領犯罪：

白領犯罪（white collar crime）係指一個人或一群人在原本受人尊敬和合法之職業或財經活動中，違反法律的行爲。通常電腦犯罪者多半爲程式設計師、系統分析師或職務上常操作電腦者，這些人多半不使用暴力，而是運用智力。加上又有社會地位，頗符合白領犯罪的型態。

2. 專業性與業務性：

實施電腦犯罪必須運用電腦專業知識，並非一般人都能完成。此外根據國外統計，絕大多數電腦犯罪都是內部員工所爲，因此大多與業務有關。

3. 損害性高：

近年來人們依賴電腦的程度頗高，很多資料具有高度機密性與重要性。如數量龐大、複雜的金額款項幾乎都交由電腦管理，一旦遭到侵害，其損害可想而知。

4. 高犯罪黑數：

犯罪黑數（dark figure of crime）乃是已發生但沒有被政府機構登錄的犯罪行爲。據美國聯邦調查局估計，認爲只有 1/100 的電腦犯罪爲人所知，而在發現的電腦犯罪案件中，只有 4/100 到達偵查機關之手。足見犯罪黑數在電腦犯罪中非常嚴重。其中最主要的原因是犯罪發生後，各企業爲顧及信譽與秘密，多半採取保密措施，或者認定係人爲操作疏失所致，而不詳加追究，才造成電腦犯罪猖獗。

5. 持續性：

通常行爲人會不只一次犯罪，而是重複再犯，或者犯行本身是一種繼續的狀態，整個案件會延續到被發覺爲止，如同刑法上的繼續犯、連續犯或常業犯。

6. 行爲與結果時間和地點之分離：

此點類似於毒害他人，通常犯罪後結果並不馬上呈現出來，只是電腦犯罪之分離時間更久，有些要經年累月（如電腦病毒）；而犯罪地點與結果地點亦分屬不同管轄，甚至跨越國界，此點又不同於大多數的犯罪型態。

7. 偵查與起訴有技術上之困難：

除了是因爲前述的高犯罪黑數外，證據取得亦十分不易。此乃是因爲檢察官或司法人員本身對電腦認識不夠外，再加上行爲與結果間隔許久，行爲人多半藏匿無蹤或得手後隨即湮滅證據，均是造成起訴困難的主因。

8.處罰太輕：

目前立法機關尚未制定出特別法來針對電腦犯罪加以處罰，僅能依一般刑案中目的相似之詐欺罪、毀損罪、侵占罪或竊盜罪等加以懲處，刑度與行爲成功後所獲得利益不成比例，如有犯罪者獲取十七萬美金不法利益，卻只判緩刑及一千美元罰金。

9.電腦兼具阻止與促進犯罪因素：

其說明了電腦犯罪中的專業性及職務性，惟有懂得電腦知識、接觸此項職務的人員才得以犯罪。但也無異提供了這些人絕佳的犯罪機會，這在其他犯罪領域中，很少會有如此兼具正反二因素的現象。

10.智慧型犯罪：

犯罪者通常受過高等教育，以高度智慧實施犯罪行爲，而非使用暴力手段。不過隨著電腦的普及和大衆化，電腦犯罪已逐漸平民化，已經不是電腦專業人員的專利。

㈢電腦犯罪之種類：

1.最早將電腦犯罪作分類者首推學者 Parker，將電腦犯罪分爲四類：

⑴犯罪的客體（object）：電腦、資料儲存體或程式成爲犯罪攻擊的目標，如破壞電腦程式或資料及偷竊硬體等。

⑵犯罪的主體（subject）：電腦成爲非常適合犯罪的獨特環境，亦即電腦系統很容易誘發犯罪，電腦程式很容易被竄改。

⑶犯罪的工具（instrument）：某些犯罪型態及方法極其複雜，需要以電腦作爲犯罪的工具，如勒索及間諜等。

⑷犯罪的象徵（symbol）：由於民衆普遍相信電腦資料的正確性，因此可能被人用來掩飾電腦詐欺或脅迫等犯罪行爲，如詐欺性電腦擇友、徵婚等。

2.美國白宮的「網路非法行爲工作小組」（President's working group on unlawful conduct on the Internet）則將電腦犯罪分爲三類：

⑴犯罪目標：如駭客入侵、恐怖主義者攻擊電腦、飛客盜打電話、阻斷服務及郵件炸彈等。

⑵儲存裝置：如盜取通行碼、信用卡號碼、專利資訊、商用軟體等。

⑶通訊工具：如利用電子郵件進行威脅、騷擾、追蹤、誘騙或散布色情圖片等行爲。

3.根據聯合國「電腦犯罪防治手冊」，將電腦犯罪分爲五類：

利用電腦的詐欺行爲、利用電腦作爲實施僞造行爲的犯罪工具、毀損或修改電腦資料或程式、非法進入他人電腦系統及服務、非法複製受法律保護之電腦軟體的行爲。

4.日本「警察白書」將電腦犯罪分爲「妨害電腦系統機能」和「不當使用電腦系統」的犯罪兩大類。

精選試題

一、電腦犯罪有何特性？電腦犯罪者的特質又為何？試分別申論之。

答：㈠電腦犯罪的特性：

1. 白領犯罪：

白領犯罪（white collar crime）係指一個人或一群人在原本受人尊敬和合法之職業或財經活動中，違反法律的行爲。通常電腦犯罪者多半爲程式設計師、系統分析師或職務上常操作電腦者，這些人多半不使用暴力，而是用智力。再加上又有社會地位，頗符合白領犯罪的型態，同時亦是智慧型犯罪的一種。

2. 損害性高：

近年來人們依賴電腦的程度頗高，很多資料具有高度機密性與重要性。如數量龐大、複雜的金額款項幾乎都交由電腦管理，一旦遭受到侵害，其損害可想而知。

3. 高犯罪黑數：

所謂犯罪黑數乃是已發生但沒有被政府機構所登錄之犯罪行爲。據美國聯邦調查局之估計，認爲只有 1/100 的電腦犯罪爲人所知；在發現之電腦犯罪案件中，只有 4/100 到達偵查機關之手。足見犯罪黑數在電腦犯罪中非常嚴重。主要原因是犯罪發生後各企業爲顧及信譽與秘密，多半採保密措施，或者僅認定係人爲操作疏失所致，而不詳加追究，才造成電腦犯罪猖獗。

4. 持續性：

電腦犯罪者通常是重複再犯，或者犯行本身是一種繼續的狀態，整個案件延續至被發覺爲止，如同刑法上之繼續犯、連續犯或常業犯。

5. 行爲與結果時間之分離：

電腦犯罪後結果並不馬上呈現出來，只是電腦犯罪之分離時間更久，此點又不同於大多數的犯罪型態。

6. 偵查與起訴有技術上之困難：

除了高犯罪黑數外，證據之取得亦十分不易；此乃是檢察官或司法人員本身對電腦認識不夠外，再加上行爲與結果間隔許久，行爲人多半藏匿無蹤或得手後隨即湮滅證據，均是造成起訴困難之主因。

7.處罰太輕：

現行立法機關尚未制定出特別法來針對電腦犯罪作處罰，僅能依一般刑案中目的相似之詐欺罪、毀損罪、侵占罪或竊盜罪等加以懲處，刑度與行爲成功後所獲得之利益不成比例。

8.電腦兼具阻止與促進犯罪因素：

電腦犯罪係屬專業性及職務性，惟有懂得電腦知識、接觸此項職務之人員才得以犯罪。但也無異提供了這些人絕佳之犯罪機會，這在其他犯罪領域中很少會有如此兼具正反二因素之現象。

㈡電腦犯罪者的特質：

1.組織特質：描述電腦犯罪者如何組織起來。

⑴組織：間諜和組織犯罪顯然組織嚴密，但電腦犯罪通常是獨自行動，甚至結構非常鬆散。

⑵召募及吸引：電腦犯罪提供許多誘惑，從貪心到尋求智力挑戰者都有，詐欺犯通常年紀較大、較成熟、受教育較高；而怪客則通常是因爲要獲得同僚對其景仰而受到吸引。

⑶國際聯繫：很多怪客和間諜人員有國際聯繫。

2.作業特質：描述電腦罪犯如何實際從事犯罪行爲。

⑴計畫：某些電腦犯罪會小心翼翼的計畫，而有些則是因爲組織沒有採取適當的預防措施而從事犯罪。

⑵技術層次：很多電腦犯罪者技術很高且見識廣博，他們花費很多時間研究和準備犯罪，反制這種威脅需要熟悉其作爲的電腦和安全專家。

⑶使用的策略和方法：策略是依據動機和技術層次而有所不同。

3.行爲特質：描述電腦犯罪者本身的特質。

⑴動機：包括金錢、開玩笑、尋求智力、挑戰和報復都有，也有可能包含兩種以上因素。

⑵個人特質：聰明、具備電腦技術、貪婪或有反文化傾向。

⑶潛在弱點：藉由犯罪者的潛在弱點可將其捕獲。

4.資源特質：描述電腦犯罪者具備或需要的資源。

⑴訓練：技巧從正式訓練或工作經驗得來。

⑵基本配備：電腦犯罪大多只需要基本的電腦設備，當然也有可能用到複雜如攔截電子通訊的設施。

⑶共犯結構：怪客有些得到同儕團體的幫忙，間諜人員則是獲得其支持政府的協助，但大多數的罪犯係獨自行動，並不需要他人協助。